

WHAT IS CLAIMED IS

5

1. A digital certificate management system comprising:

a client and server system in which a digital certificate is used for authentication so as to
10 establish communication between a server and a client, and data transmission is performed therebetween with the use of the communication established through the authentication; and

a digital certificate management apparatus
15 communicatable with the client and the server, and

wherein:

said digital certificate management apparatus comprises a proof key updating unit which updates a proof key used for proving validity of the digital
20 certificate used for authentication by the server;

said proof key updating unit comprises:

a unit configured to acquire a new proof key for updating;

a unit configured to acquire a new digital
25 certificate used for the authentication for which

validity can be proved with the use of said new proof key;

a first transmitting unit transmitting the new proof key to the client; and

5 a second transmitting unit transmitting a new server certificate which is the new digital certificate for the server, to the server, and

wherein:

said second transmitting unit performs
10 operation of transmitting the new server certificate to the server after receiving, from the client, information indicating that the client has received the new proof key.

15

2. The digital certificate management system as claimed in claim 1, wherein:

20 said proof key updating unit in said digital certificate management apparatus comprises a unit configured to acquire a proof key certificate, which is a digital certificate, including the new proof key, for which validity can be proved with the use of an old
25 proof key, and

wherein:

said first transmitting unit is configured to transmit the new proof key in a form of the proof key certificate to the client; and

5 said client comprises a unit configured to be responsive to the proof key included in the proof key certificate transmitted from said digital certificate management apparatus, for proving validity of the received proof key certificate with the use of the old
10 proof key and storing the proof key included in the proof key certificate when determining that the proof key is a proper one.

15

3. The digital certificate management system as claimed in claim 1, wherein:

said proof key updating unit in the digital
20 certificate management system comprises:

a unit configured to acquire a first proof key certificate, including the new proof key, which is a digital certificate for which validity can be proved with the use of an old proof key; and

25 a unit configured to acquire a second proof

key certificate, including the new proof key, which is a digital certificate for which validity can be proved with the use of the new proof key, and

wherein:

5 said first transmitting unit is configured to transmit the new proof keys in respective forms of the first proof key certificate and the second proof key certificate to the client; and

 said client comprises:

10 a unit configured to be responsive to the first proof key certificate transmitted from said digital certificate management apparatus, for proving validity of the received certificate with the use of the old proof key and storing the certificate when
15 determining that it is a proper one; and

 a unit configured to be responsive to the second proof key certificate from said digital certificate management apparatus, for proving validity of the received certificate with the use of the new
20 proof key included in the first proof key certificate, and storing the second proof key certificate when determining that it is a proper one, and then deleting the old proof key certificate and the first proof key certificate, and

25 wherein:

the first transmitting unit in the digital certificate management apparatus is configured to perform operation of transmitting the second proof key certificate to the client at least after receiving
5 information from the server indicating that the server has received the new server certificate.

10

4. A digital certificate management system comprising:

a client and server system in which a digital certificate is used for mutual authentication so as to
15 establish communication between a server and a client, and data transmission is performed therebetween with the use of the communication established through the authentication; and

a digital certificate management apparatus
20 communicatable with the client and the server, and

wherein:

said digital certificate management apparatus comprises a proof key updating unit which updates a proof key used for proving validity of the digital
25 certificate used for the mutual authentication by the

client and the server;

said proof key updating unit comprises:

a unit configured to acquire a new proof key
for updating;

5 a unit configured to acquire a new digital
certificate used for the mutual authentication for which
validity can be proved with the use of said new proof
key;

10 a first transmitting unit transmitting a new
client certificate which is the new digital certificate
for the client, and the new proof key, to the client;
and

15 a second transmitting unit transmitting a new
server certificate which is the new digital certificate
for the server, and the new proof key, to the server,
and

wherein:

20 said second transmitting unit performs
operation of transmitting the new server certificate to
the server after receiving from, the client, information
indicating that the client has received the new proof
key; and

25 said first transmitting unit performs
operation of transmitting the new client certificate to
the client after receiving information from the server

indicating that the server has received the new proof key.

5

5. The digital certificate management system as claimed in claim 4, wherein:

said first transmitting unit is configured to
10 transmit the new proof key at the same time of or in
prior to transmission of the new client certificate to
the client; and

said second transmitting unit is configured to
transmit the new proof key at the same time of or in
15 prior to transmission of the new server certificate to
the server.

20

6. A digital certificate management system comprising:

a client and server system in which a digital
certificate is used for mutual authentication so as to
25 establish communication between a server and a client,

and data transmission is performed therebetween with the use of the communication established through the authentication; and

a digital certificate management apparatus
5 communicatable with the client and the server, and
wherein:

said digital certificate management apparatus
comprises a proof key updating unit which updates a
proof key used for proving validity of the digital
10 certificate used for the mutual authentication by the
client and the server;

said proof key updating unit comprises:

a unit configured to acquire a new proof key
for updating;

15 a unit configured to acquire a new digital
certificate used for the mutual authentication for which
validity can be proved with the use of said new proof
key;

a first transmitting unit transmitting a new
20 client certificate which is the new digital certificate
for the client, and the new proof key, to the client;
and

a second transmitting unit transmitting a new
server certificate which is the new digital certificate
25 for the server, and the new proof key, to the server,

and

wherein:

said first transmitting unit performs
operation of transmitting the new client certificate and
5 the new proof key to the client at the same time; and

said second transmitting unit performs
operation of transmitting the new server certificate and
the new proof key to the server at the same time after
receiving information from the client indicating that
10 the client has received the new proof key.

15 7. The digital certificate management system
as claimed in claim 1, wherein:

said server has an intermediary function for
communication between the digital certificate management
apparatus and the client;

20 said digital certificate management apparatus
and the client perform data transmission mutually via
the server; and

the server transmits the new proof key and/or
the new client certificate to the client, transmitted
25 from the first transmitting unit of the digital

certificate management apparatus for the client, via the communication established through authentication performed with the client with the use of an old digital certificate.

5

8. The digital certificate management system
10 as claimed in claim 4, wherein:

said server has an intermediary function for communication between the digital certificate management apparatus and the client;

said digital certificate management apparatus
15 and the client perform data transmission mutually via the server; and

the server transmits the new proof key and/or the new client certificate to the client, transmitted from the first transmitting unit of the digital
20 certificate management apparatus for the client, via the communication established through authentication performed with the client with the use of an old digital certificate.

25

9. The digital certificate management system as claimed in claim 6, wherein:

said server has an intermediary function for communication between the digital certificate management apparatus and the client;

said digital certificate management apparatus and the client perform data transmission mutually via the server; and

the server transmits the new proof key and/or the new client certificate to the client, transmitted from the first transmitting unit of the digital certificate management apparatus for the client, via the communication established through authentication performed with the client with the use of an old digital certificate.

10. The digital certificate management system as claimed in claim 1, wherein:

said client has an intermediary function for communication between the digital certificate management apparatus and the server;

said digital certificate management apparatus

and the server perform data transmission mutually via the client; and

the client transmits the new proof key and/or the new server certificate to the server, transmitted
5 from the second transmitting unit of the digital certificate management apparatus for the server, via the communication established through authentication performed with the server with the use of an old digital certificate.

10

11. The digital certificate management
15 system as claimed in claim 4, wherein:

said client has an intermediary function for communication between the digital certificate management apparatus and the server;

said digital certificate management apparatus
20 and the server perform data transmission mutually via the client; and

the client transmits the new proof key and/or the new server certificate to the server, transmitted from the second transmitting unit of the digital
25 certificate management apparatus for the server, via the

communication established through authentication performed with the server with the use of an old digital certificate.

5

12. The digital certificate management system as claimed in claim 6, wherein:

10 said client has an intermediary function for communication between the digital certificate management apparatus and the server;

 said digital certificate management apparatus and the server perform data transmission mutually via
15 the client; and

 the client transmits the new proof key and/or the new server certificate to the server, transmitted from the second transmitting unit of the digital certificate management apparatus for the server, via the
20 communication established through authentication performed with the server with the use of an old digital certificate.

25

13. The digital certificate management system
as claimed in claim 1, wherein:

the authentication performed between the
client and the server comprises authentication according
5 to an SSL or TLS protocol; and

the server certificate comprises a public key
certificate for the server.

10

14. The digital certificate management system
as claimed in claim 4, wherein:

the authentication performed between the
15 client and the server comprises authentication according
to an SSL or TLS protocol; and

the server certificate comprises a public key
certificate for the server.

20

15. The digital certificate management system
as claimed in claim 6, wherein:

25 the authentication performed between the

client and the server comprises authentication according to an SSL or TLS protocol; and

the server certificate comprises a public key certificate for the server.

5

16. A digital certificate management
10 apparatus communicatable with a client and a server which configure a client and server system, comprising:

a proof key updating unit which updates a proof key used for proving validity of a digital certificate used by the server for authentication
15 through which communication between the client and the server is established, and

wherein:

said proof key updating unit comprises:

a unit configured to acquire a new proof key
20 for updating;

a unit configured to acquire a new digital certificate used for the authentication for which validity can be proved with the use of said new proof key;

25 a first transmitting unit transmitting the new

proof key to the client; and

a second transmitting unit transmitting a new server certificate which is the new digital certificate for the server to the server, and

5 wherein:

 said second transmitting unit performs operation of transmitting the new server certificate to the server after receiving, from the client, information indicating that the client has received the new proof
10 key.

15 17. A digital certificate management apparatus communicatable a client and a server which configure a client and server system, comprising:

 a proof key updating unit which updates a proof key used for proving validity of a digital
20 certificate used for mutual authentication through which communication is established between the client and the server, and

 wherein:

 said proof key updating unit comprises:

25 a unit configured to acquire a new proof key

for updating;

a unit configured to acquire a new digital certificate used for the mutual authentication for which validity can be proved with the use of said new proof

5 key;

a first transmitting unit transmitting a new client certificate which is the new digital certificate for the client, and the new proof key, to the client; and

10 a second transmitting unit transmitting a new server certificate which is the new digital certificate for the server, and the new proof key, to the server, and

wherein:

15 said second transmitting unit performs operation of transmitting the new server certificate to the server after receiving, from the client, information indicating that the client has received the new proof key; and

20 said first transmitting unit performs the operation of transmitting the new client certificate to the client after receiving information from the server indicating that the server has received the new proof key.

25

18. A digital certificate management apparatus communicatable with a client and a server which configure a client and server system, comprising:

5 a proof key updating unit which updates a proof key used for proving validity of a digital certificate used for mutual authentication through which communication is established between the client and the server, and wherein:

said proof key updating unit comprises:

10 a unit configured to acquire a new proof key for updating;

a unit configured to acquire a new digital certificate used for the mutual authentication for which validity can be proved with the use of said new proof
15 key;

a first transmitting unit transmitting a new client certificate which is the new digital certificate for the client, and the new proof key, to the client; and

20 a second transmitting unit transmitting a new server certificate which is the new digital certificate for the server, and the new proof key, to the server, and

wherein:

25 said first transmitting unit performs

operation of transmitting the new client certificate and the new proof key to the client at the same time; and

5 said second transmitting unit performs operation of transmitting the new server certificate and the new proof key to the server at the same time after receiving information from the client indicating that the client has received the new proof key.

10

19. A digital certificate management system comprising:

15 a client and server system in which one or a plurality of clients and one or a plurality of servers are included, authentication is performed between each client and each sever with the use of a digital certificate, and data transmission is performed therebetween with communication established through the authentication; and

20 a digital certificate management apparatus communicatable with each client and each server, and

 wherein:

 said digital certificate management apparatus
25 comprises:

a proof key updating unit updating a proof key used for proving validity of the digital certificate used for authentication by each server; and

an updating order control unit controlling a
5 procedure of updating the proof key performed by the proof key updating unit based on information concerning respective nodes included in the client and server system as to a communication counterpart of each node and as to whether each of the node and the counterpart
10 acts as a client or a server, and

wherein:

said proof key updating unit comprises:

a unit configured to acquire a new proof key for updating;

15 a unit configured to acquire a new digital certificate used for the authentication for which validity can be proved with the use of said new proof key;

a first transmitting unit transmitting the new
20 proof key to each client; and

a second transmitting unit transmitting a new server certificate which is the new digital certificate for each server, to the relevant server, and

wherein:

25 said updating order control unit controls the

updating procedure so that said second transmitting unit performs operation of transmitting the new server certificate to the respective server after receiving from all the clients, which act as communication counterparts of the server, information indicating that the clients have received the new proof keys.

10

20. The digital certificate management system as claimed in claim 19, wherein:

said proof key updating unit in said digital certificate management apparatus comprises a unit configured to acquire a proof key certificate, including the new proof key, which is a digital certificate for which validity can be proved with the use of an old proof key, and

wherein:

20 said first transmitting unit is configured to transmit the new proof key in a form of the proof key certificate, to each client; and

each client comprises a unit configured to be responsive to the proof key certificate transmitted from said digital certificate management apparatus, for

25

proving validity of the received proof key certificate with the use of the old proof key and storing the proof key included in the proof key certificate when determining that the proof key is a proper one.

5

21. The digital certificate management system
10 as claimed in claim 19, wherein:

said proof key updating unit in the digital certificate management system comprises:

a unit configured to acquire a first proof key certificate, including the new proof key, which is a
15 digital certificate for which validity can be proved with the use of an old proof key; and

a unit configured to acquire a second proof key certificate, including the new proof key, which is a digital certificate for which validity can be proved
20 with the use of the new proof key, and

wherein:

said first transmitting unit is configured to transmit the new proof keys in respective forms of the first proof key certificate and the second proof key
25 certificate to each client; and

each client comprises:

a unit configured to be responsive to the first proof key certificate transmitted from said digital certificate management apparatus, for proving
5 validity of the received certificate with the use of the old proof key and storing the certificate when determining that it is a proper one; and

a unit configured to be responsive to the second proof key certificate transmitted from said
10 digital certificate management apparatus, for proving validity of the received certificate with the use of the new proof key included in the first proof key certificate, and storing the second proof key certificate when determining that it is a proper one,
15 and then deleting the old proof key certificate and the first proof key certificate, and

wherein:

the updating order control unit in the digital certificate management apparatus is configured to
20 perform control such that the operation of transmitting the second proof key certificate to each client from the first transmitting unit is performed at least after receiving information from all the servers which act as communication counterparts of the client indicating that
25 the servers have received the new server certificates.

22. A digital certificate management system comprising:

a client and server system in which one or a plurality of clients and one or a plurality of servers
5 are included, mutual authentication is performed between each client and each sever with the use of a digital certificate, and data transmission is performed therebetween with communication established through the authentication; and

10 a digital certificate management apparatus communicatable with each client and each server, and

wherein:

said digital certificate management apparatus comprises:

15 a proof key updating unit which updates a proof key used for proving validity of the digital certificate used for the mutual authentication by each client and each server; and

an updating order control unit controlling a
20 procedure of updating the proof key performed by the proof key updating unit based on information concerning the respective nodes included in the client and server system as to a communication counterpart of each node and as to whether each of the node and the counterpart
25 acts as a client or a server, and

wherein:

said proof key updating unit comprises:

a unit configured to acquire a new proof key
for updating;

5 a unit configured to acquire a new digital
certificate, used for the mutual authentication, for
which validity can be proved with the use of said new
proof key;

 a first transmitting unit transmitting a new
10 client certificate which is the new digital certificate
for each client, and the new proof key, to the relevant
client; and

 a second transmitting unit transmitting a new
server certificate which is the new digital certificate
15 for each server, and the new proof key, to the relevant
server, and

wherein:

 said updating order control unit controls the
updating procedure so that said second transmitting unit
20 performs the operation of transmitting the new server
certificate to each server after receiving, from all the
clients which act as communication counterparts of the
relevant server, information indicating that the
relevant clients have received the new proof keys, and
25 said first transmitting unit performs the operation of

transmitting the new client certificate to each client
after receiving information, from all the servers which
act as communication counterparts of the relevant client,
indicating that the relevant servers have received the
5 new proof keys.

10 23. A digital certificate management system
comprising:

 a client and server system in which one or a
plurality of clients and one or a plurality of servers
are included, mutual authentication is performed between
15 each client and each sever with the use of a digital
certificate, and data transmission is performed
therebetween with communication established through the
authentication; and

 a digital certificate management apparatus
20 communicatable with each client and each server, and

 wherein:

 said digital certificate management apparatus
comprises:

 a proof key updating unit which updates a
25 proof key used for proving validity of the digital

certificate used for the mutual authentication by each client and each server; and

an updating order control unit controlling a procedure of updating the proof key performed by the
5 proof key updating unit based on information concerning the respective nodes included in the client and server system as to a communication counterpart of each node and as to whether each of the node and the counterpart acts as a client or a server, and

10 wherein:

said proof key updating unit comprises:

a unit configured to acquire a new proof key for updating;

a unit configured to acquire a new digital
15 certificate used for the mutual authentication for which validity can be proved with the use of said new proof key;

a first transmitting unit transmitting a new client certificate which is the new digital certificate
20 for each client, and the new proof key, to the client; and

a second transmitting unit transmitting a new server certificate which is the new digital certificate for each server, and the new proof key, to the server,
25 and

wherein:

said updating order control unit controls the updating procedure so that said first transmitting unit performs the operation of transmitting the new client
5 certificate and the new proof key to each client at the same time, and said second transmitting unit performs the operation of transmitting the new server certificate and the new proof key to each server at the same time after receiving information, from all the clients which
10 act as communication counterparts of the relevant server, indicating that the clients have received the new proof keys.

15

24. The digital certificate management system as claimed in claim 19, wherein:

each server has an intermediary function for
20 communication between the digital certificate management apparatus and at least one of the clients;

said digital certificate management apparatus and each of said at least one client perform data transmission mutually via any of the servers; and

25 the server transmits the new proof key and/or

the new client certificate to the client, transmitted
from the first transmitting unit of the digital
certificate management apparatus for the client, via the
communication established through authentication
5 performed with the client, which is a transmission
destination, with the use of an old digital certificate.

10

25. The digital certificate management system
as claimed in claim 22, wherein:

each server has an intermediary function for
communication between the digital certificate management
15 apparatus and at least one of the clients;

said digital certificate management apparatus
and each of said at least one client perform data
transmission mutually via any of the servers; and

the server transmits the new proof key and/or
20 the new client certificate to the client, transmitted
from the first transmitting unit of the digital
certificate management apparatus for the client, via the
communication established through authentication
performed with the client, which is a transmission
25 destination, with the use of an old digital certificate.

26. The digital certificate management system as claimed in claim 23, wherein:

each server has an intermediary function for communication between the digital certificate management apparatus and at least one of the clients;

said digital certificate management apparatus and each of said at least one client perform data transmission mutually via any of the servers; and

the server transmits the new proof key and/or the new client certificate to the client, transmitted from the first transmitting unit of the digital certificate management apparatus for the client, via the communication established through authentication performed with the client, which is a transmission destination, with the use of an old digital certificate.

27. The digital certificate management system as claimed in claim 19, wherein:

each client has an intermediary function for communication between the digital certificate management apparatus and at least one of the servers;

said digital certificate management apparatus

and each of said at least one server perform data
transmission mutually via any of the clients; and

the client transmits the new proof key and/or
the new server certificate to the server, transmitted
5 from the second transmitting unit of the digital
certificate management apparatus for the server, via the
communication established through authentication
performed with the server, which is a transmission
destination, with the use of an old digital certificate.

10

28. The digital certificate management system
15 as claimed in claim 22, wherein:

each client has an intermediary function for
communication between the digital certificate management
apparatus and at least one of the servers;

said digital certificate management apparatus
20 and each of said at least one server perform data
transmission mutually via any of the clients; and

the client transmits the new proof key and/or
the new server certificate to the server, transmitted
from the second transmitting unit of the digital
25 certificate management apparatus for the server, via the

communication established through authentication performed with the server, which is a transmission destination, with the use of an old digital certificate.

5

29. The digital certificate management system as claimed in claim 23, wherein:

10 each client has an intermediary function for communication between the digital certificate management apparatus and at least one of the servers;

 said digital certificate management apparatus and each of said at least one server perform data
15 transmission mutually via any of the clients; and

 the client transmits the new proof key and/or the new server certificate to the server, transmitted from the second transmitting unit of the digital certificate management apparatus for the server, via the
20 communication established through authentication performed with the server. which is a transmission destination, with the use of an old digital certificate.

25

30. The digital certificate management system
as claimed in claim 19, wherein:

the authentication performed between the
client and the server comprises authentication according
5 to an SSL or TLS protocol; and

the server certificate comprises a public key
certificate for the server.

10

31. The digital certificate management system
as claimed in claim 22, wherein:

the authentication performed between the
15 client and the server comprises authentication according
to an SSL or TLS protocol; and

the server certificate comprises a public key
certificate for the server.

20

32. The digital certificate management system
as claimed in claim 23, wherein:

25 the authentication performed between the

client and the server comprises authentication according to an SSL or TLS protocol; and

the server certificate comprises a public key certificate for the server.

5

33. A digital certificate management
10 apparatus communicatable with one or a plurality of clients and one or a plurality of servers which configure a client and server system, comprising:

a proof key updating unit updating a proof key used for proving validity of a digital certificate used
15 for authentication by the server, whereby communication is established between each client and each server; and

an updating order control unit controlling a procedure of updating the proof key performed by the proof key updating unit based on information concerning
20 the respective nodes included in the client and server system as to a communication counterpart of each node and as to whether each of the node and the counterpart acts as a client or a server, and

wherein:

25 said proof key updating unit comprises:

a unit configured to acquire a new proof key
for updating;

a unit configured to acquire a new digital
certificate used for the authentication for which
5 validity can be proved with the use of said new proof
key;

a first transmitting unit transmitting the new
proof key to each client; and

a second transmitting unit transmitting a new
10 server certificate which is the new digital certificate
for each server, to the relevant server, and

wherein:

said updating order control unit controls the
updating procedure so that second transmitting unit
15 performs the operation of transmitting the new server
certificate to the respective server after receiving
from all the clients, which act as communication
counterparts of the server, information indicating that
the clients have received the new proof keys.

20

34. A digital certificate management
25 apparatus communicatable with one or a plurality of

clients and one or a plurality of servers which
configure a client and server system, comprising:

5 a proof key updating unit updating a proof key
used for proving validity of a digital certificate used
for mutual authentication, whereby communication is
established between each client and each server; and

an updating order control unit controlling a
procedure of updating the proof key performed by the
proof key updating unit based on information concerning
10 the respective nodes included in the client and server
system as to a communication counterpart of each node
and as to whether each of the node and the counterpart
acts as a client or a server, and

wherein:

15 said proof key updating unit comprises:

a unit configured to acquire a new proof key
for updating;

a unit configured to acquire a new digital
certificate, used for the mutual authentication, for
20 which validity can be proved with the use of said new
proof key;

a first transmitting unit transmitting a new
client certificate which is the new digital certificate
for each client, and the new proof key, to the relevant
25 client; and

a second transmitting unit transmitting a new server certificate which is the new digital certificate for each server, and the new proof key, to the relevant server, and

5 wherein:

 said updating order control unit controls the updating procedure so that said second transmitting unit performs the operation of transmitting the new server certificate to each server after receiving, from all the
10 clients which act as communication counterparts of the relevant server, information indicating that the relevant clients have received the new proof keys, and said first transmitting unit performs the operation of transmitting the new client certificate to each client
15 after receiving information, from all the servers which act as communication counterparts of the relevant client, indicating that the relevant servers have received the new proof keys.

20

35. A digital certificate management apparatus communicatable with one or a plurality of
25 clients and one or a plurality of servers which

configure a client and server system, comprising:

5 a proof key updating unit updating a proof key
used for proving validity of a digital certificate used
for mutual authentication, whereby communication is
established between each client and each server; and

an updating order control unit controlling a
procedure of updating the proof key performed by the
proof key updating unit based on information concerning
the respective nodes included in the client and server
10 system as to a communication counterpart of each node
and as to whether each of the node and the counterpart
acts as a client or a server, and

wherein:

said proof key updating unit comprises:

15 a unit configured to acquire a new proof key
for updating;

a unit configured to acquire a new digital
certificate used for the mutual authentication for which
validity can be proved with the use of said new proof
20 key;

a first transmitting unit transmitting a new
client certificate which is the new digital certificate
for each client, and the new proof key, to the client;
and

25 a second transmitting unit transmitting a new

server certificate which is the new digital certificate for each server, and the new proof key, to the server, and

wherein:

5 said updating order control unit controls the updating procedure so that said first transmitting unit performs the operation of transmitting the new client certificate and the new proof key to each client at the same time, and said second transmitting unit performs
10 the operation of transmitting the new server certificate and the new proof key to each server at the same time after receiving information, from all the clients which act as communication counterparts of the relevant server, indicating that the clients have received the new proof
15 keys.

20 36. A digital certificate management method for managing, in a digital certificate management apparatus communicatable with a server and a client which configure a client and server system, a digital certificate used for authentication whereby
25 communication is established between the server and the

client, comprising the steps of:

a) updating a proof key used for proving validity of the digital certificate used for authentication by the server, and

5 wherein said step a) comprises the steps of:

a-1) acquiring a new proof key for updating;
and

a-2) acquiring a new digital certificate used for the authentication for which validity can be proved
10 with the use of said new proof key;

b-1) transmitting the new proof key to the client; and

b-2) transmitting a new server certificate which is a new digital certificate for the server, to
15 the server, after receiving, from the client, information indicating that the client has received the new proof key.

20

37. The digital certificate management method as claimed in claim 36, wherein:

said step a) further comprises the step of a-
25 3) acquiring a proof key certificate, which is the

digital certificate, including the new proof key, for which validity can be proved with the use of an old proof key;

said step b-1) comprises the step of b-3)
5 transmitting the new proof key in a form of the proof key certificate to the client; and

when the proof key certificate is transmitted to the client, the client is caused to prove validity of the received proof key certificate with the use of the
10 old proof key and store the proof key included in the proof key certificate when determining that the proof key is a proper one.

15

38. The digital certificate management method as claimed in claim 36, wherein:

said step a) further comprises the steps of:
20 a-4) acquiring a first proof key certificate, including the new proof key, which is the digital certificate for which validity can be proved with the use of an old proof key; and
a-5) acquiring a second proof key certificate,
25 including the new proof key, which is a digital

certificate for which validity can be proved with the use of the new proof key, and

wherein:

said step b-1) comprises the step of
5 transmitting the new proof keys in respective forms of the first proof key certificate and the second proof key certificate to the client;

after the completion of said step b-2), the second proof key certificate is transmitted to the
10 client at least after information indicating that the server has received the new server certificate is received;

the client is caused to prove validity of the received certificate with the use of the old proof key
15 upon receiving the first proof key certificate, and to store the certificate when determining that it is a proper one; and

the client is caused to prove validity of the received certificate with the use of the new proof key
20 included in the first proof key certificate when receiving the second proof key certificate, and to store the second proof key certificate when determining that it is a proper one, and then delete the old proof key certificate and the first proof key certificate.

25

39. A digital certificate management method for managing, in a digital certificate management apparatus communicatable with a server and a client which configure a client and server system, a digital
5 certificate used for mutual authentication whereby communication is established between the server and the client, comprising the steps of:

a) updating a proof key used for proving validity of the digital certificate used for the mutual
10 authentication by the client and the server, and

wherein:

said step a) comprises the steps of;

a-1) acquiring a new proof key for updating;

and

15 a-2) acquiring a new digital certificate used for the mutual authentication for which validity can be proved with the use of said new proof key;

b-1) transmitting the new proof key to the server;

20 b-2) transmitting the new proof key to the client;

b-3) transmitting a new client certificate which is the new digital certificate for the client, to the client; and

25 b-4) transmitting a new server certificate

which is the new digital certificate for the server, to the server; and

wherein:

said steps a-1), a-2), b-1), b-2), b-3) and b-
5 4) are executed in a predetermined order; and

said step b-4) is performed after the
completion of said step b-2) and also after information
indicating that the client has received the new proof
key from the client is received from the client, and
10 also, said step b-3) is performed after the completion
of said step b-1) and also after information indicating
that the server has received the new proof key is
received from the server.

15

40. The digital certificate management method
as claimed in claim 39, wherein:

20 said step b-3) is performed at the same time
or after the completion of said step b-2), and also,
said step b-4) is performed at the same time or after
the completion of said step b-1).

25

41. A digital certificate management method for managing, in a digital certificate management apparatus communicatable with a server and a client which configure a client and server system, a digital
5 certificate used for mutual authentication whereby communication is established between the server and the client, comprising the steps of:

a) updating a proof key used for proving validity of the digital certificate used for the mutual
10 authentication by the client and the server, and

wherein:

said step a) comprises the steps of;

a-1) acquiring a new proof key for updating;

a-2) acquiring a new digital certificate used
15 for the mutual authentication for which validity can be proved with the use of said new proof key;

b-1) transmitting the new proof key to the server;

b-2) transmitting the new proof key to the
20 client;

b-3) transmitting a new client certificate which is the new digital certificate for the client, to the client; and

b-4) transmitting a new server certificate
25 which is the new digital certificate for the server, to

the server, and

wherein:

said steps a-1), a-2), b-1), b-2), b-3) and b-4) are executed in a predetermined order; and

5 said steps b-2) and b-3) are performed together, and then, after the completion of these steps and after information indicating that the client has received the new proof key, said steps b-1) and b-4) are performed together.

10

42. The digital certificate management method
15 as claimed in claim 36, wherein:

said digital certificate management apparatus and the client perform data transmission mutually via the server; and

the server transmits the new proof key and/or
20 the new client certificate to the client, transmitted in said step b-2) and/or said step b-3) from the digital certificate management apparatus for the client, via the communication established through authentication performed with the client with the use of an old digital
25 certificate.

43. The digital certificate management method as claimed in claim 39, wherein:

said digital certificate management apparatus and the client perform data transmission mutually via
5 the server; and

the server transmits the new proof key and/or the new client certificate to the client, transmitted in said step b-2) and/or said step b-3) from the digital certificate management apparatus for the client, via the
10 communication established through authentication performed with the client with the use of an old digital certificate.

15

44. The digital certificate management method as claimed in claim 41, wherein:

said digital certificate management apparatus
20 and the client perform data transmission mutually via the server; and

the server transmits the new proof key and/or the new client certificate to the client, transmitted in said step b-2) and/or said step b-3) from the digital
25 certificate management apparatus for the client, via the

communication established through authentication performed with the client with the use of an old digital certificate.

5

45. The digital certificate management method as claimed in claim 36, wherein:

10 said digital certificate management apparatus and the server perform data transmission mutually via the client; and

 the client transmits the new proof key and/or the new server certificate to the server, transmitted in
15 said step b-1) and/or said step b-4) from the digital certificate management apparatus for the server, via the communication established through authentication performed with the server with the use of an old digital certificate.

20

46. The digital certificate management method
25 as claimed in claim 39, wherein:

said digital certificate management apparatus and the server perform data transmission mutually via the client; and

the client transmits the new proof key and/or
5 the new server certificate to the server, transmitted in
said step b-1) and/or said step b-4) from the digital
certificate management apparatus for the server, via the
communication established through authentication
performed with the server with the use of an old digital
10 certificate.

15 47. The digital certificate management method
as claimed in claim 41, wherein:

said digital certificate management apparatus
and the server perform data transmission mutually via
the client; and

20 and the client transmits the new proof key
and/or the new server certificate to the server,
transmitted in said step b-1) and/or said step b-4) from
the digital certificate management apparatus for the
server, via the communication established through
25 authentication performed with the server with the use of

an old digital certificate.

5

48. The digital certificate management method
as claimed in claim 36, wherein:

the authentication performed between the
client and the server comprises authentication according
10 to an SSL or TLS protocol; and

the server certificate comprises a public key
certificate for the server.

15

49. The digital certificate management method
as claimed in claim 39, wherein:

the authentication performed between the
20 client and the server comprises authentication according
to an SSL or TLS protocol; and

the server certificate comprises a public key
certificate for the server.

25

50. The digital certificate management method
as claimed in claim 41, wherein:

the authentication performed between the
client and the server comprises authentication according
5 to an SSL or TLS protocol; and

the server certificate comprises a public key
certificate for the server.

10

51. A digital certificate management method
for managing, in a digital certificate management
apparatus communicatable with one or a plurality of
15 servers and one or a plurality of clients which
configure a client and server system, a digital
certificate used for mutual authentication whereby
communication is established between the one or the
plurality of servers and the one or the plurality of
20 clients, comprising the steps of:

a) updating a proof key used for proving
validity of the digital certificate used for
authentication, based on an updating procedure
determined according to information concerning the
25 respective nodes included in the client and server

system as to a communication counterpart of each node and as to whether each of the node and the counterpart acts as a client or a server, and

wherein:

5 said step a) comprising the steps of:

 a-1) acquiring a new proof key for updating;

 a-2) acquiring a new digital certificate used for the mutual authentication for which validity can be proved with the use of said new proof key;

10 a-3) transmitting the new proof key to each client; and

 a-4) transmitting a new server certificate which is a new digital certificate for each server, to the server, and

15 wherein:

 said updating procedure is configured so that said step a-4) is performed after information indicating that the new proof keys have been received is received from all the clients, which act as communication

20 counterparts of the relevant server.

25 52. The digital certificate management method

as claimed in claim 51, wherein:

said step a) further comprises the steps of a-
5) acquiring a proof key certificate, including the new
proof key, which is the digital certificate for which
5 validity can be proved with the use of an old proof key,
and

wherein:

said step a-3) comprises the step of
transmitting the new proof key in a form of the proof
10 key certificate to the client; and

the client is caused to prove validity of the
received proof key certificate with the use of the old
proof key when receiving the proof key certificate, and
to store the proof key included in the proof key
15 certificate when determining that the proof key is a
proper one.

20

53. The digital certificate management method
as claimed in claim 51, wherein:

said step a) further comprises the step of:
a-6) acquiring a first proof key certificate,
25 including the new proof key, which is the digital

certificate for which validity can be proved with the use of an old proof key; and

a-7) acquiring a second proof key certificate, including the new proof key, which is the digital
5 certificate for which validity can be proved with the use of the new proof key, and

wherein:

said step a-3) comprises the step of transmitting the new proof keys in respective forms of
10 the first proof key certificate and the second proof key certificate to each client;

said step a) is configured so that the operation of transmitting the second proof key certificate to each client is performed at least after
15 information is received from all the servers, which act as communication counterparts of the client, indicating that the servers have received the new server certificate;

each client is caused to be responsive to the
20 first proof key certificate received from said digital certificate management apparatus, for proving validity of the received certificate with the use of the old proof key and storing the certificate when determining that it is a proper one; and

25 each client is caused to be responsive to the

second proof key certificate received from said digital
certificate management apparatus for proving validity of
the received certificate with the use of the new proof
key included in the first proof key certificate and
5 storing the second proof key certificate when
determining that it is a proper one, and then to delete
the old proof key certificate and the first proof key
certificate.

10

54. A digital certificate management method
for managing, in a digital certificate management
15 apparatus communicatable with one or a plurality of
servers and one or a plurality of clients which
configure a client and server system, a digital
certificate used for mutual authentication whereby
communication is established between the one or the
20 plurality of servers and the one or the plurality of
clients, comprising the step of:

a) updating a proof key used for proving
validity of the digital certificate used for the mutual
authentication based on an updating procedure determined
25 according to information concerning the respective nodes

included in the client and server system as to a communication counterpart of each node and as to whether each of the node and the counterpart acts as a client or a server, and

5 wherein:

 said step a) comprises:

 a-1) acquiring a new proof key for updating;

 a-2) acquitting a new digital certificate,
used for the mutual authentication, for which validity
10 can be proved with the use of said new proof key;

 a-3) transmitting a new client certificate
which is the new digital certificate for each client,
and the new proof key, to the relevant client; and

 a-4) transmitting a new server certificate
15 which is the new digital certificate for each server,
and the new proof key, to the relevant server, and

 wherein:

 said updating procedure is configured so that
said step a-4) is performed after information indicating
20 that the relevant clients have received the new proof
keys is received from all the clients which act as
communication counterparts of the relevant server, and
said step a-3) is performed after information indicating
that the relevant servers have received the new proof
25 keys is received from all the servers which act as

communication counterparts of the relevant client.

5

55. A digital certificate management method for managing, in a digital certificate management apparatus communicatable with one or a plurality of servers and one or a plurality of clients which
10 configure a client and server system, a digital certificate used for mutual authentication whereby communication is established between the one or the plurality of servers and the one or the plurality of clients, comprising the step of:

15 a) updating a proof key used for proving validity of the digital certificate used for the mutual authentication based on an updating procedure determined according to information concerning the respective nodes included in the client and server system as to a
20 communication counterpart of each node and as to whether each of the node and the counterpart acts as a client or a server, and

wherein:

said step a) comprises the steps of:

25 a-1) acquiring a new proof key for updating;

a-2) acquiring a new digital certificate used for the mutual authentication for which validity can be proved with the use of said new proof key;

a-3) transmitting a new client certificate
5 which is the new digital certificate for each client, and the new proof key, to the client; and

a-4) transmitting a new server certificate which is the new digital certificate for each server, and the new proof key, to the server, and

10 wherein said updating procedure is configured so that operations of transmitting the new client certificate and the new proof key to each client are performed at the same time, and operations of transmitting the new server certificate and the new
15 proof key to each server are performed at the same time after information indicating that the clients have received the new proof keys is received from all the clients which act as communication counterparts of the relevant server.

20

56. The digital certificate management method
25 as claimed in claim 51, wherein:

said digital certificate management apparatus and each client perform data transmission mutually via any of the servers; and

the server transmits the new proof key and/or
5 the new client certificate to the client, transmitted from the digital certificate management apparatus for the client in said step a-3), via the communication established through authentication performed with the client which is a transmission destination with the use
10 of an old digital certificate.

15 57. The digital certificate management method as claimed in claim 54, wherein:

said digital certificate management apparatus and each client perform data transmission mutually via any of the servers; and

20 the server transmits the new proof key and/or the new client certificate to the client, transmitted from the digital certificate management apparatus for the client in said step a-3), via the communication established through authentication performed with the
25 client which is a transmission destination with the use

of an old digital certificate.

5

58. The digital certificate management method
as claimed in claim 55, wherein:

said digital certificate management apparatus
and each client perform data transmission mutually via
10 any of the servers; and

the server transmits the new proof key and/or
the new client certificate to the client, transmitted
from the digital certificate management apparatus for
the client in said step a-3), via the communication
15 established through authentication performed with the
client which is a transmission destination with the use
of an old digital certificate.

20

59. The digital certificate management method
as claimed in claim 51, wherein:

said digital certificate management apparatus
25 and each server perform data transmission mutually via

any of the clients; and

the client transmits the new proof key and/or
the new server certificate to the server, transmitted
from the digital certificate management apparatus for
5 the server in said step a-4), via the communication
established through authentication performed with the
server which is a transmission destination with the use
of an old digital certificate.

10

60. The digital certificate management method
as claimed in claim 54, wherein:

15 said digital certificate management apparatus
and each server perform data transmission mutually via
any of the clients; and

the client transmits the new proof key and/or
the new server certificate to the server, transmitted
20 from the digital certificate management apparatus for
the server in said step a-4), via the communication
established through authentication performed with the
server which is a transmission destination with the use
of an old digital certificate.

25

61. The digital certificate management method as claimed in claim 55, wherein:

said digital certificate management apparatus and each server perform data transmission mutually via
5 any of the clients; and

the client transmits the new proof key and/or the new server certificate to the server, transmitted from the digital certificate management apparatus for the server in said step a-4), via the communication
10 established through authentication performed with the server which is a transmission destination with the use of an old digital certificate.

15

62. The digital certificate management method as claimed in claim 51, wherein:

the authentication performed between the
20 client and the server comprises authentication according to an SSL or TLS protocol; and

the server certificate comprises a public key certificate for the server.

25

63. The digital certificate management method
as claimed in claim 54, wherein:

the authentication performed between the
client and the server comprises authentication according
5 to an SSL or TLS protocol; and

the server certificate comprises a public key
certificate for the server.

10

64. The digital certificate management method
as claimed in claim 55, wherein:

the authentication performed between the
15 client and the server comprises authentication according
to an SSL or TLS protocol; and

the server certificate comprises a public key
certificate for the server.

20

65. An updating procedure determining method
for determining an updating procedure to be stored in
25 one or a plurality of clients and one or a plurality of

servers which configure a client and server system, for
updating by a digital certificate management apparatus a
proof key used for proving validity of a digital
certificate used for authentication, through which
5 communication is established between the one or the
plurality of clients and the one or the plurality of
servers, comprising the step of:

determining the updating procedure based on
information concerning the respective nodes included in
10 the client and server system as to a communication
counterpart of each node and as to whether each of the
node and the counterpart acts as a client or a server,

so that a step of transmitting a new server
certificate which is the new digital certificate for
15 which validity can be proved with the use of a new proof
key for updating, used for the authentication by the
server, is performed after information indicating that
all the clients which act as communication counterparts
of the server is received from the clients.

20

66. A program for causing a computer, which
25 controls a digital certificate management apparatus

communicatable with a client and a server which
configure a client and server system, to perform a proof
key updating step of updating a proof key used for
providing validity of a digital certificate used by the
5 server for authentication performed when communication
is established between the client and the server, said
program being configured to cause the computer to
function as:

10 a unit configured to acquire a new proof key
for updating;

a unit configured to acquire a new digital
certificate used for the authentication for which
validity can be proved with the use of said new proof
key;

15 a first transmitting unit transmitting the new
proof key to the client; and

a second transmitting unit transmitting a new
server certificate which is the new digital certificate
for the server, to the server, and

20 wherein:

said second transmitting unit performs the
operation of transmitting the new server certificate to
the server after receiving from the client information
indicating that the client has received the new proof
25 key.

67. A program for causing a computer, which controls a digital certificate management apparatus communicatable with a client and a server which configure a client and server system, to perform a proof
5 key updating step of updating a proof key used for providing validity of a digital certificate used for authentication performed when communication is established between the client and the server, said program being configured to cause the computer to
10 function as:

a unit configured to acquire a new proof key for updating;

a unit configured to acquire a new digital certificate used for the mutual authentication for which
15 validity can be proved with the use of said new proof key;

a first transmitting unit transmitting a new client certificate which is the new digital certificate for the client, and the new proof key, to the client;
20 and

a second transmitting unit transmitting a new server certificate which is the new digital certificate for the server, and the new proof key, to the server,
and

25 wherein:

said second transmitting unit performs the operation of transmitting the new server certificate to the server after receiving from the client information indicating that the client has received the new proof
5 key; and

said first transmitting unit performs the operation of transmitting the new client certificate to the client after receiving information from the server indicating that the server has received the new proof
10 key.

15 68. A program for causing a computer, which controls a digital certificate management apparatus communicatable with a client and a server which configure a client and server system, to perform a proof key updating step of updating a proof key used for
20 proving validity of a digital certificate used for authentication performed when communication is established between the client and the server, said program being configured to cause the computer to function as:

25 a unit configured to acquire a new proof key

for updating;

a unit configured to acquire a new digital certificate used for the mutual authentication for which validity can be proved with the use of said new proof

5 key;

a first transmitting unit transmitting a new client certificate which is the new digital certificate for the client, and the new proof key, to the client; and

10 a second transmitting unit transmitting a new server certificate which is the new digital certificate for the server, and the new proof key, to the server, and

wherein:

15 said first transmitting unit has a function of performing the operation of transmitting the new client certificate and the new proof key to the client at the same time; and

20 said second transmitting unit has a function of performing the operation of transmitting the new server certificate and the new proof key to the server at the same time after receiving information from the client indicating that the client has received the new proof key.

25

69. A program for causing a computer, which controls a digital certificate management apparatus communicatable with one of a plurality of clients and one or a plurality of servers which configure a client and server system, to function as:

a proof key updating unit updating a proof key used for proving validity of a digital certificate used for authentication by each server for establishing communication between each server and each client; and

10 an updating order control unit controlling a procedure of updating the proof key performed by the proof key updating unit based on information concerning the respective nodes included in the client and server system as to a communication counterpart of each node and as to whether each of the node and the counterpart acts as a client or a server, and

wherein:

said proof key updating unit comprises:

a unit configured to acquire a new proof key
20 for updating;

a unit configured to acquire a new digital certificate used for the authentication for which validity can be proved with the use of said new proof key;

25 a first transmitting unit transmitting the new

proof key to each client; and

a second transmitting unit transmitting a new server certificate which is the new digital certificate for each server, to the relevant server, and

5 wherein:

said updating order control unit controls the updating procedure so that said second transmitting unit performs the operation of transmitting the new server certificate to the respective server after receiving
10 from all the clients, which act as communication counterparts of the server, information indicating that the clients have received the new proof keys.

15

70. A program for causing a computer, which controls a digital certificate management apparatus communicatable with one of a plurality of clients and
20 one or a plurality of servers which configure a client and server system, to function as:

a proof key updating unit updating a proof key used for proving validity of the digital certificate used for mutual authentication for establishing
25 communication between each server and each client; and

an updating order control unit controlling a procedure of updating the proof key performed by the proof key updating unit based on information concerning the respective nodes included in the client and server
5 system as to a communication counterpart of each node and as to whether each of the node and the counterpart acts as a client or a server, and

wherein:

said proof key updating unit has the functions
10 of:

a unit configured to acquire a new proof key for updating;

a unit configured to acquire a new digital certificate, used for the mutual authentication, for
15 which validity can be proved with the use of said new proof key;

a first transmitting unit transmitting a new client certificate which is the new digital certificate for each client, and the new proof key, to the relevant
20 client; and

a second transmitting unit transmitting a new server certificate which is the new digital certificate for each server, and the new proof key, to the relevant server, and

25 wherein:

said updating order control unit is configured to control the updating procedure so that said second transmitting unit performs the operation of transmitting the new server certificate to each server after
5 receiving, from all the clients which act as communication counterparts of the relevant server, information indicating that the relevant clients have received the new proof keys, and said first transmitting unit performs the operation of transmitting the new
10 client certificate to each client after receiving information, from all the servers which act as communication counterparts of the relevant client, indicating that the relevant servers have received the new proof keys.

15

71. A program for causing a computer, which
20 controls a digital certificate management apparatus communicatable with one of a plurality of clients and one or a plurality of servers which configure a client and server system, to function as:

a proof key updating unit updating a proof key
25 used for proving validity of the digital certificate

used for mutual authentication for establishing
communication between each server and each client; and

an updating order control unit controlling a
procedure of updating the proof key performed by the
5 proof key updating unit based on information concerning
the respective nodes included in the client and server
system as to a communication counterpart of each node
and as to whether each of the node and the counterpart
acts as a client or a server, and

10 wherein:

said proof key updating unit has the functions
of:

a unit configured to acquire a new proof key
for updating;

15 a unit configured to acquire a new digital
certificate used for the mutual authentication for which
validity can be proved with the use of said new proof
key;

a first transmitting unit transmitting a new
20 client certificate which is the new digital certificate
for each client, and the new proof key, to the client;
and

a second transmitting unit transmitting a new
server certificate which is the new digital certificate
25 for each server, and the new proof key, to the server,

and

wherein:

said updating order control unit is configured
to control the updating procedure so that said first
5 transmitting unit performs the operations of
transmitting the new client certificate and the new
proof key to each client at the same time, and said
second transmitting unit performs the operations of
transmitting the new server certificate and the new
10 proof key to each server at the same time after
receiving information, from all the clients which act as
communication counterparts of the relevant server,
indicating that the clients have received the new proof
keys.

15

72. A computer readable information recording
20 medium storing therein the program claimed in claim 66.

25 73. A computer readable information recording

medium storing therein the program claimed in claim 67.

5

74. A computer readable information recording medium storing therein the program claimed in claim 68.

10

75. A computer readable information recording medium storing therein the program claimed in claim 69.

15

76. A computer readable information recording medium storing therein the program claimed in claim 70.

20

77. A computer readable information recording medium storing therein the program claimed in claim 71.